A New Heuristic Approach to Safeguarding Online Digital Data

P.V. Raj Varma[1], M.Rajinikanth[2], Dr. Mohammed Ali Hussain[3]

[1]Pursuing M.Tech, Dept. of Computer Science Engineering, Sri Sunflower College of Engineering & Technology, A.P., India.

[2]Assoc. Professor, Dept. of Computer Science Engineering, Sri Sunflower College of Engineering & Technology, A.P., India.

[3]Professor, Dept. of Computer Science Engineering, Sri Sai Madhavi Institute of Science & Technology, A.P., India.

Abstract: *Security challenges have been raised by private and public sectors related to exchange digital data electronically. In the current state, protocols such as the simple mail transfer protocol (SMTP), post office protocol (POP), and internet message access protocol (IMAP) transfer and store email messages in plaintext. Therefore, the confidentiality of email messages cannot be assured. Email sent using these protocols and without using any other security tool, must be assumed to have been read and compromised, because its confidentiality and integrity cannot be assured. Thus in this paper a new approach as a tool for improvement of current popular email protocols is proposed. The novel proposed protocol will be manifested in the Email Security Protocol (ESP) which is designed to add a layer of security and confidentiality to email messages transmitted over unsecured public networks. ESP is designed in three models to allow efficient and effective implementation upon various information system architectures. The result of testing the new proposed approach showed superior performance comparing to the existing one.*

Keywords *- Electronic Email, Digital data, Protocol, Security Tool.*

I. Introduction

Email has become an integral part of today's digital life. Individual send and receive a vast mass of email messages every day. However, email is one of the most insecure types of communication media. Common configurations of email clients enable attackers to steal user names and passwords used to access email easily. The content of Web-based email Not encrypted and is passed in the network in plain text. Messages deleted from an email server might Still be retrievable from other servers halfway around the world without owner knowledge. This paper presents email security issues and proposes a new tool on how to improve email systems security. The rest of the paper is divided into the following sections. Second, background which presents the current state of email security protocols . Third, the need for a new protocol which presents the challenges of the exiting protocols throughout two cases. Fourth, the new approach which presents its descriptions and features and the fifth is the conclusion and future research.

II. Background

There are currently a number of email protocols in use. Some of these are the simple mail transfer protocol (SMTP), post office protocol (POP), and internet message access protocol (IMAP) [5]. The SMTP and POP protocols are very popular protocols and are used by many who use email.

A typical person likely has their email program configured to send and receive email using the SMTP and POP protocols. The main reason for this is because their internet service provider (ISP) or email service provider uses these protocols and in order for the email program to communicate with the email server, their program needs to be configured to use these protocols. The SMTP protocol is used when sending email and the POP protocol is used when receiving email.

Internet message access protocol (IMAP) is similar to POP but allows email to remain on the server [6]. The email remains on the server until the user specifically deletes them from the server. Furthermore, with the use of IMAP, email has the ability to be organized on the server and accessed from any computer with access to the internet.

A major drawback of these protocols in terms of information security is the lack of protection that is provided to email that is transmitted and received. Email is transmitted in plaintext and confidentiality and integrity are nearly non-existent. For example, email servers communicate with each other using SMTP and store email messages in plain, unencrypted text [5].

III. Need For A New Protocol

There is a need for email security protocols and tools to protect the confidentiality and integrity of email. Without any form of encryption in place, email transmitted in plaintext over unsecured networks must be assumed to have been read and compromised because of the ease and ability adversaries have in using network protocol analyzers (sniffers) to capture traffic on unsecured networks. Mark Vanden wauver and Frank Jorissen demonstrate the need for security measures in their paper titled Securing Internet Electronic Mail [8]. The authors state that "Each message can be intercepted by a trained computer user connected to the net … using tools to check the functionality of the network (Protocol Analyzers also known as network sniffers) which also can be used to listen in on any traffic on the internet."

Another example that demonstrates the need for enhanced email security protocols is given by Marvin Cetron and Owen Davies in their article titled Ten Critical Trends for Cyber security. The major theme of the paper states "Technological advances and greater connectivity may be making our systems less rather than more secure. A special panel of military, intelligence, and forecasting experts analyzes the trends that may be leading the world to cyberwar." Since electronic mail travels over the same networks as other packets of information, this topic includes email and should be a major concern to organizations and corporations that value the confidentiality of their electronic communications and information. Furthermore, if email communications are not adequately secure, adversaries gain the ability to compromise the confidentiality and integrity of email, which in turn allows them to collect information from these communications that can be brought together to gain enough proprietary information to launch a larger and more damaging attack against an organization. Secure email transmission through the use of a tool such as the Email Security Protocol can reduce the risks of such an event from occurring by securing email and making it unreadable and unusable to adversaries that may intercept it in transit.

IV. Esp Proposed Protocol

The security problems associated with the SMTP, POP, and IMAP protocols warrants the consideration of a new protocol that would eliminate some of the security risks associated with using these protocols. This protocol would be used for the secure transmission of email from one person to another through a public network (i.e., internet). Furthermore, this protocol is shown to protect the confidentiality of email that travels from one SMTP server to another while on its way to its intended recipient.

The proposed name for this protocol is the email security protocol (ESP). Its purpose is to add a layer of security and confidentiality to email in which it is used. The ESP is configured and implemented in an email program so that its functions are carried out automatically with minimal interaction with the user being required.

A. ESP ACHITECTURE

The Email Security Protocol (ESP) is designed in three models to allow efficient and effective implementation upon various information system architectures. Model I is designed based on a single server architecture which will process the encryption and the decryption procedures. It would be good on a network system isolated from the internet. The main feature of this model is that the email would stay encrypted on the server until the recipient decided to retrieve them. The email would thus be secure while being stored on the server. This model could also be used in a simulation in a computer laboratory; especially if the number of available servers for research is limited.

B. ESP PROCESS:

ESP uses asymmetric encryption to encrypt the contents of email messages before they are transmitted to the SMTP server. In this manner, the contents and subject line of an email message are encrypted and are protected from adversaries that otherwise would have been able to read the email in its plaintext. Thus, a major benefit is provided by the use of the ESP because if used properly, there is an assurance that email messages have been transmitted with confidentiality intact.

The email is encrypted using the public key (PK) of the recipient. A feature of the ESP is that if the PK of the recipient is unknown, then an automatic request for the PK will be sent to the recipient. When the recipient receives this request, and if the email program is configured correctly and also using the ESP, then the PK is automatically returned to the sender. Then the email can be encrypted using the PK and securely transmitted through the gamut of SMTP servers and maintain its confidentiality while in route to its intended recipient.

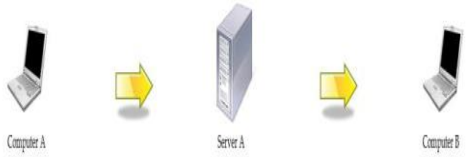


Figure1: Model Architecture

Model II is designed to be used with the architecture associated with several servers and via the internet cloud. It would be good for sending email from one internal network system (corporation) to another. Its main feature is that the email would be secure in transit (encrypted) over the internet (public domain) from Server to another. This would greatly enhance the security of email sent from one corporation to another; or from one corporation to the same corporation with offices at a different geographical location.

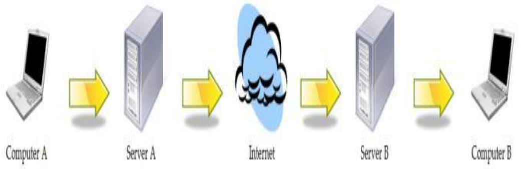


Figure2: Model II Architecture

Model III is designed based on the Internet cloud architecture and for sending encrypted email directly from one computer to another. This model will serve better when an internal network server is not present or used for email traffic. It is main feature is that the email would be encrypted and secure from one computer to another; encryption would be present for the entire trip over the networks, including the internet.

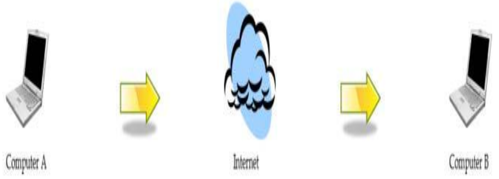


Figure3: Model III Architecture

For simplicity, Alice and Bob will be the entities used in describing the transfer of email from one person to the other. Traditionally in cryptography texts, Alice and Bob have been denoted as good guys [6]. A more detailed description of how the ESP will work can best be illustrated in the following scenario.

Alice desires to send an email to Bob using ESP. Alice also knows that Bob is using ESP. However, Alice does not have Bob's public key (PK). Since Alice does not know Bob's PK, the process will take three emails (steps) to be completed. After Alice finishes composing the email she intends to send to Bob, she clicks the send button on her email program.

A feature of the email security protocol is that the process takes place automatically and an asymmetrically encrypted email may be sent to a recipient whose public key had previously been unknown. Also, under the correct circumstances, this process can be completed very quickly. Also, most importantly, the contents of the email message remains secure while in transit through the internet and the gamut of SMTP servers until it reaches its intended destination; email messages are asymmetrically encrypted before being transmitted. The confidentiality of the email has been preserved through the use of the ESP. Furthermore, the convenience of an automatic and secure process makes for ease of use.

C. Esp Advantages And Drawbacks

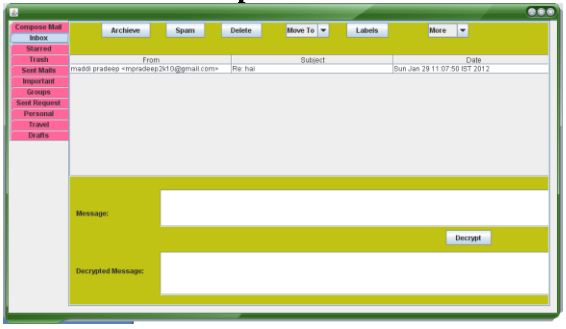
An advantage of the ESP is the ease of use for the end users. For example, in an organization that has a local area network (LAN) administered by information technology (IT) personnel, the IT staff can install and configure the ESP as needed, depending on the model used (I, II, or III), on the required computers, workstations, and servers that make up the LAN. Once the ESP is properly configured, users can send and receive email as they normally would and have the assurance that their email will be (1) securely (encrypted) stored on the server until retrieved by the intended recipient, (2) securely transmitted from one ESP configured server to another (e.g., one corporate office to another), or (3) securely transmitted from one ESP configured computer to another. If a combination of models I, II, and III are used then security can be provided at all of the above mentioned levels.

Another advantage is the transparency to the user. The user will not be required to perform any extra steps or manually execute and run any special program for the ESP to work properly on their computer. Once properly configured, the ESP will run in the background and automatically perform the required tasks as needed, depending on the configuration and model used. The user will not have to worry about forgetting to encrypt their email transmissions because the ESP will perform the task automatically for them. This eliminates the risk of human error and gives confidence that all email transmissions from a particular computer or server are secure.

A drawback of the ESP is that in order for the encryption and secure transmission of email to take place, the servers and computers need to be properly configured. If they are not configured correctly, then the secure transmission of email will not be able to take place.

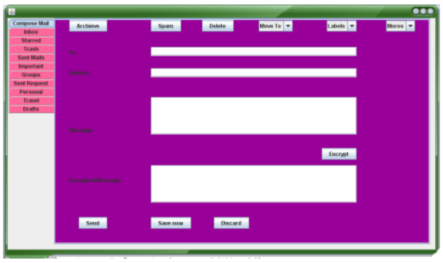
Another drawback with the ESP is that it mainly provides security from outside threats. For example, in model II email transmissions are secure in their travel over the internet from server A to server B; server A being one regional organization office and server B being another regional organization office. Once the email is requested for retrieval by computer B (recipient), then the email is transmitted in plaintext inside the LAN to computer B. There is a risk that an inside threat can intercept this email. However, by using a combination of models II and III, this drawback and risk can be eliminated.

V. Experimental results Inbox

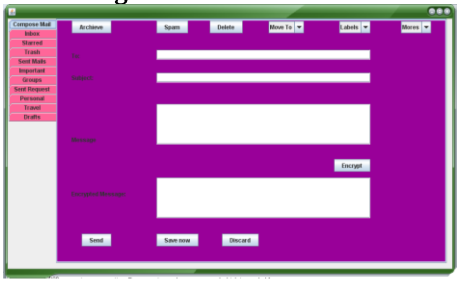


From	Subject	Date
maddi pradeep <mpradeep2k10@gmail.com>	Re: hai	Sun Jan 29 11:07:50 IST 2012

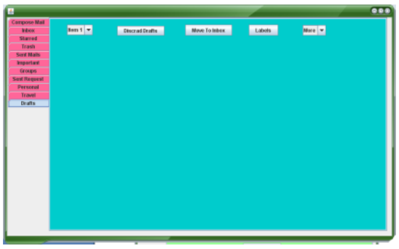
Sending Mails



Encryption Message



Drafts



VI. Conclusion And Future Research

It has been shown that the new proposed protocol (ESP) would be an enhancement and great email security tool to preserve the confidentiality of email messages in transit over the internet. Furthermore, it is evident that it provides a high degree of security which includes email securely stored on a server. Our future research is to investigate the ESP in depth using a large scale of data and advance it to eliminate any drawback.

References

[1] Behrouz A. Forouzan, Cryptography and Network Security, McGraw Hill, 2008.

[2] Mark Stamp, Information Security: Principles and Practices, Wiley, 2006.

[3] http://email-security.net/papers/usablesecure- email.pdf.

[4] http://email-security.net/papers/takefive.html.

[5] Richard Sinn, Software Security Technologies: A Programmatic Approach, Thomson Course Technology, 2008.

[6] Mark Ciampa, Security+ Guide to Network Security Fundamentals, Course Technology, 2009.

[7] Jiangtao Li, Ninghui Li, William Winsborough, "Automated Trust Negotiation Using Cryptographic Credentials", ACM Transactions on Information and System Security, Vol. 13, No. 1, Article 2, Publication date: October 2009.

[8] Mark Vandenwauver and Frank Jorissen. Securing Internet Electronic Mail. In State of the Art in Applied Cryptography, Course on Computer Security and Industrial Cryptography - Revised Lectures, Bart Preneel and Vincent Rijmen (Eds.). Springer-Verlag, London, UK, 1997. 208-223.